

ABSTRACT OF THE DISCLOSURE

A method and apparatus for securely establishing voice over Internet Protocol calls are disclosed. In a Registration Security approach, a Gatekeeper sends an Access Token in all Registration Request messages. The Access Token contains information that authenticates the Gateway to the Gatekeeper. The Gatekeeper formats a message to an authentication server that will authenticate the information contained in the token, and the server responds with either an Access-Accept or Access-Reject message. The Gatekeeper responds to the Gateway with either a Registration Confirm message or a Registration Reject message. If a call is then placed from a successfully authenticated Gateway, that Gateway generates a new Access Token that is identical to the one generated during registration, except for the timestamp. The Gatekeeper uses the authentication server to authenticate the originating gateway, before sending the designation side Access Confirm message. As a result, a non-authenticated endpoint that knows a Gateway's address cannot use the Gateway address to circumvent security and access the telephone network to place unauthorized calls or free calls. In Admission or Per-Call Security, a Gateway is also required to include an Access Token in all originating side Admission Request messages. Such token contains information that identifies the user of the Gateway to the Gatekeeper, based on an account number and PIN obtained from the user. The Access Token is authenticated in the manner described above.